Afrekenen met pc-paranoia

13 fabeltjes doorprikt

Internetten, surfen, mailen, zelfs gewoon een brief schrijven op je computer kan hem naar de verdoemenis helpen... zeggen ze. We worden soms onterecht bang gemaakt over zaken die kunnen fout lopen op internet of op je pc. Er zijn heel wat zaken die we gerust als 'urban legends' of 'hoaxes' mogen catalogeren. Clickx vertelt je waarvan je zeker niét bang hoeft te zijn. FREDERICK GORDTS

Ben je een geoefend computergebruiker en word je wel eens aangeklampt voor het oplossen van bepaalde problemen? Dan krijg je ongetwijfeld ook onwaarschijnlijke verhalen te horen van collega's, vrienden of kennissen. Misschien is het ook niets meer dan een een 'urban legend' of een 'hoax' – Engels voor bedrog, mop of grap – om iemand te foppen of beet te nemen. Clickx ging op zoek naar de meest hardnekkige urban legends, zowel online, op internet, als offline, op je eigen computer.

1 Zonder screensaver gaat je monitor stuk

Waarschijnlijk heb je het ook al eens gehoord: als je vergeet een screensaver op te zetten, kan je je monitor beschadigen. Dat klopte... in de jaren tachtig! Zonder screensaver kan een scherm wel degelijk 'inbranden', maar enkel en alleen als je weken, maanden of jaren aan een stuk hetzelfde programma laat openstaan. Kijk maar eens naar het scherm van een geldautomaat: daar blijft een bepaald deel van het scherm (het logo van de bank bijvoorbeeld) vaak altijd staan. Maar bij gewoon computergebruik is daar geen sprake van: je gebruikt nooit alleen maar één programma. Als je 's nachts je pc (of scherm) uitzet, dan heb je geen screensaver nodig. En als je een plat lcd-scherm hebt, is de kans nog kleiner dat je last krijgt van zo'n ingebrand scherm.

➲ Dus: een screensaver gebruik je vooral voor je plezier, of om ervoor te zorgen dat anderen niet kunnen zien wat je aan het doen was als je even afwezig bent.

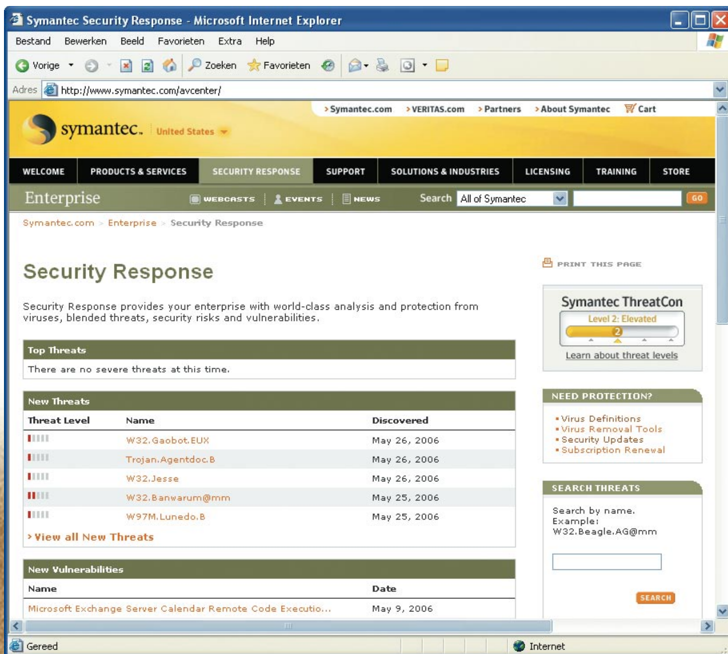


Vandaag gebruik je screensavers gewoon voor de fun.

2 Virussen wissen al je gegevens

Er zijn tienduizenden virussen in omloop, maar de overgrote meerderheid daarvan doet weinig kwaad. Ja, je systeem werkt misschien wat trager, en wellicht wordt het virus doorgestuurd naar anderen via je e-mailprogramma, maar de meeste virussen zullen je harde schijf niet wissen – gelukkig maar. Als je pc raar begint te doen, installeer dan snel een virusscanner, en de kans is groot dat het virus zonder problemen weer verwijderd kan worden en dat je geen gegevens kwijtraakt.

➲ Maar een computer zonder virusscanner raden wij niet aan! Houd de scanner ook steeds up-to-date door bijgewerkte virusdefinities te (laten) downloaden.



De meeste virussen wissen geen gegevens!

3 Te veel aan-uit is slecht voor je pc



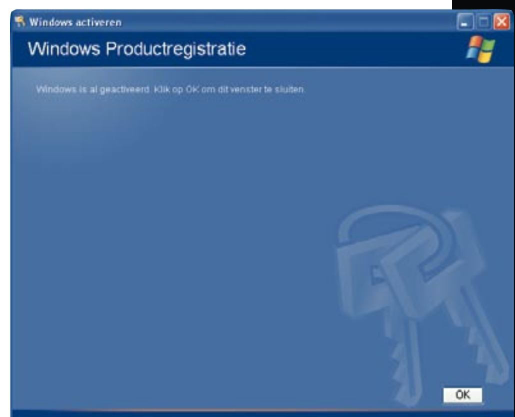
Ook de stroomschakelaar gebruiken, kan geen kwaad.

Een computer werkt net als een auto: te vaak de motor uit- en dan weer aanzetten, is niet gezond. Dat hoor je vaak zeggen. Misschien was dat een tiental jaren geleden het geval, maar nu in elk geval niet meer: de voeding (power supply) in een moderne pc is een hoogstaand stukje hardware. Elke voeding kan duizenden keren worden aan- of afgezet. En dat je stroom zou besparen door de pc niet te veel uit te zetten, is eveneens een fabeltje: je bespaart veel meer stroom als de pc uit staat.

➲ Een tip: vertrek je voor een week of langer met vakantie, zet dan je pc uit met de stroomschakelaar achteraan. Sommige pc's verbruiken namelijk nog stroom als ze uit staan, maar als je de schakelaar op nul zet, verbruiken ze niets meer. Heeft je pc geen schakelaar, trek dan gewoon de stekker uit.

4 Als je je pc upgradet, moet je een nieuwe Windows kopen

Tijd om je pc te upgraden? Misschien heb je wel net een nieuwe grafische kaart, harde schijf of zelfs processor gekocht. Je hebt gehoord dat je dan een nieuwe versie van Windows moet kopen. Klopt niet! Windows bevat wel een Productactivatiesysteem, dat zal detecteren dat je nieuwe hardware geïnstalleerd hebt. Als de wijzigingen niet te groot zijn, is er niets aan de hand. Maar als je bijvoorbeeld je moederbord hebt (moeten) vervangen, dan zal Windows wel klagen. Maar geen probleem: je kan gewoon via internet je Windows-versie opnieuw activeren. Lukt dat niet, dan kan je naar een gratis Microsoft-telefoonnummer bellen, waar je meteen een nieuwe code krijgt... als je Windows legaal hebt aangeschaft, welteverstaan!

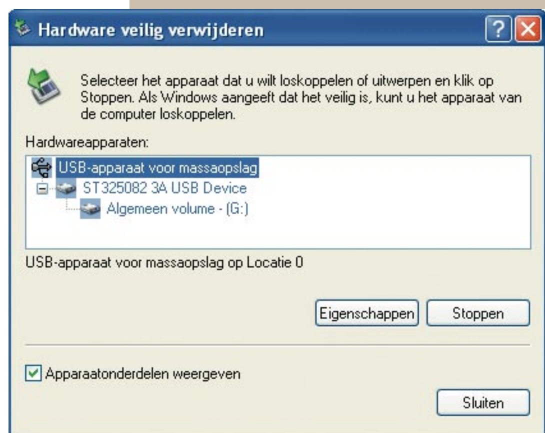


De Productactivatie van Windows heeft geen problemen met nieuwe hardware.

5 Apparaten loskoppelen is gevaarlijk

Heb jij ook randapparatuur die gebruikt maakt van usb? Usb mag dan wel plug-and-play zijn, toch wijzen veel fabrikanten erop dat je het apparaat pas mag ontkoppelen als de pc uit staat. Ze vermelden dan dat het apparaat stuk kan gaan als je het wel doet. Ook dat is een fabeltje! Geen enkel apparaat zal stuk gaan door de usb-stekker (of zelfs de stroomstekker) uit te trekken. Het enige wat kan gebeuren, is dat je gegevens verliest – in het geval van een externe harde schijf bijvoorbeeld. Ook een externe cd-schrijver ontkoppel je best niet als je een cd aan het branden bent. Sommige harde schijven schrijven trouwens nog data nadat je een bestand gekopieerd hebt. Wacht dus best een paar seconden.

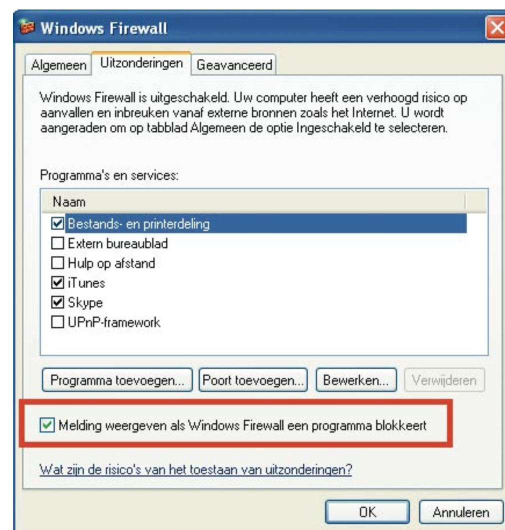
➲ Ben je niet zeker? Gebruik dan de wizard **Hardware veilig verwijderen** in het systeemvak, rechts onderaan bij het klokje. Dubbelklik op het icoontje met de groene pijl, duid het apparaat aan dat je wil verwijderen en klik op **Stoppen**. Windows laat je meteen weten wanneer je het apparaat – veilig – kan verwijderen. Maar nogmaals: dit hoeft niet voor randapparatuur als printers, scanners of modems!



Een usb-apparaat veilig loskoppelen.

6 De firewall heeft altijd gelijk

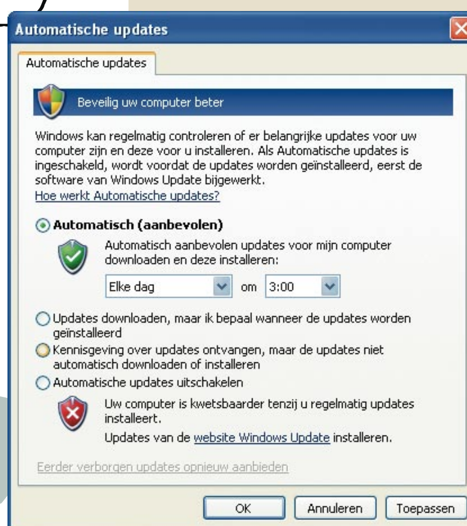
Heb je de raad van Clickx opgevolgd en gebruik je ook een firewall als ZoneAlarm of de ingebouwde Windows Firewall in Windows XP? Goed! Maar je moet niet panikeren als zo'n firewall je soms een venstertje met een gevaarlijk uitziend bericht laat zien. Omdat een goede firewall zowel binnenkomende als uitgaande pakketjes controleert, kan het zijn dat je zo'n waarschuwing krijgt na de installatie van een nieuw programma. Dan is het volkomen normaal dat de firewall je vraagt of het pakketje wel buiten (of binnen) mag. Ook als je een programma hebt geïnstalleerd dat binnenkomende pakketjes nodig heeft, zoals downloadsoftware of Skype, is dat normaal. En sommige programma's identificeren zicht erg cryptisch naar de firewall toe. Ben je niet zeker, sluit het programma dan af, start het weer op, en ga na of je opnieuw dezelfde melding van de firewall krijgt. Is dat inderdaad het geval, dan zit je goed.



Een firewall kan heel wat berichten weergeven.

7 Windows is onveilig

Heb je een Linux- of Mac-freak in je vriendenkring? Dan zal hij (of zij) je te pas en te onpas wel vertellen hoe onveilig Windows wel is: al die virussen, spyware, adware, enzovoort. Het klopt dat de meeste virussen enkel op Windows bestaan, en dat er soms ook 'beveiligingsgaten' in het besturingssysteem zitten. Maar als je je Windows goed up-to-date houdt, zal je daar geen last van hebben. Ga gewoon regelmatig naar **http://windowsupdate.microsoft.com** en download alle nieuwe software. Of beter nog, laat Windows dat automatisch doen: ga naar **Start**, **Configuratiescherm**, **Automatische updates** en kies **Automatisch**. Windows checkt de Update-server elke dag en installeert ook meteen de updates. Zo ben je steeds veilig. Let wel op: een goede virusscanner (en firewall) mogen niet ontbreken!



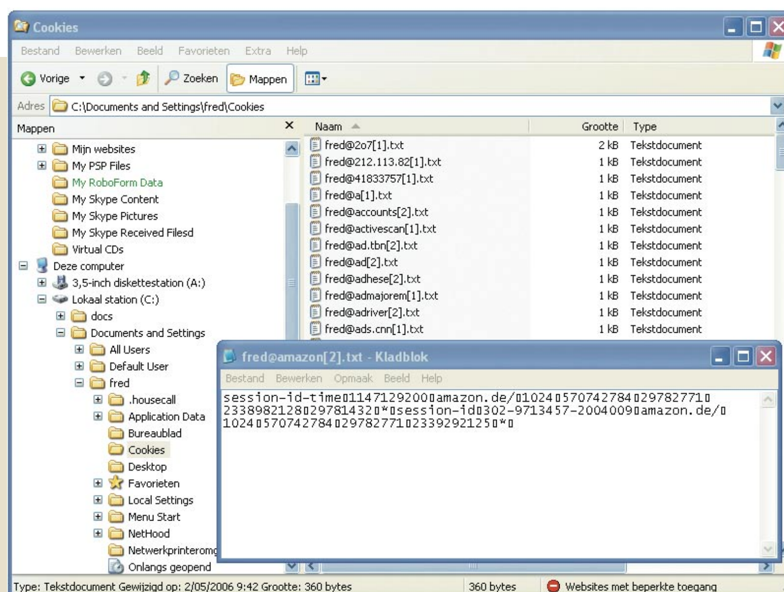
Laat Windows zichzelf updaten.



8 Cookies schenden je privacy

Cookies zijn heel kleine tekstbestandjes die door bepaalde websites op je harde schijf worden gezet. Een cookie zorgt er bijvoorbeeld voor dat je niet opnieuw je gebruikersnaam moet ingeven op een webmailsite, of dat je niet opnieuw moet inloggen om een andere pagina van een site te bezoeken. Cookies worden niet gebruikt om je creditcardgegevens op te slaan! Ze zorgen er gewoon voor dat je makkelijker en sneller kan surfen. Elke cookie is een tekstbestand dat je (als je met Internet Explorer surft) terugvindt in de map **C:\Documents and Settings\gebruikersnaam\Cookies**. Cookies hebben vaak als naam het adres van de website, zodat een onverlaat wel kan zien naar welke sites je gesurft hebt.

➲ Wil je dit niet, verwijder dan de cookies via **Internet-opties, Cookies verwijderen.** Je zal dan wel alle gebruikersnamen opnieuw moeten ingeven.



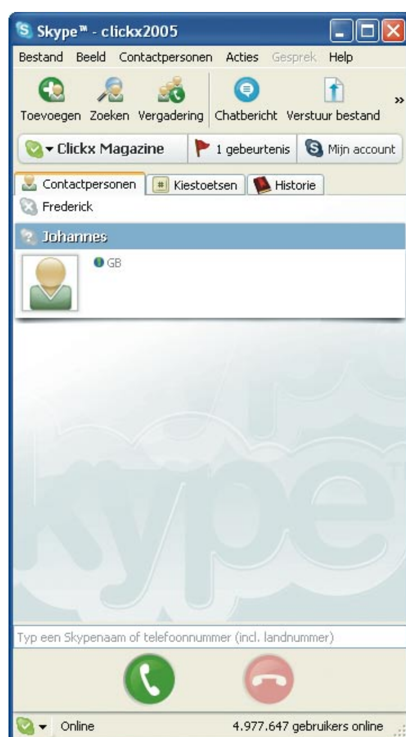
Een cookie is een onschuldig tekstbestandje.



9 Big brother kijkt mee

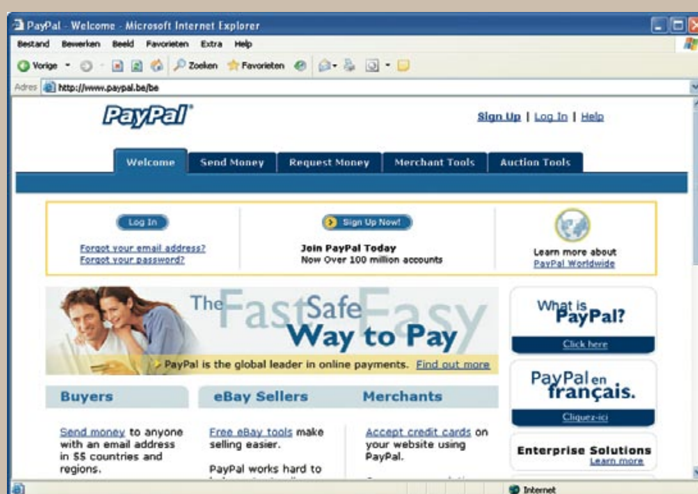
Denk jij ook dat de staatsveiligheid, de FBI of de CIA al je mailtjes lezen of je surfactiviteiten in de gaten houden? De kans is klein, erg klein! Er worden namelijk dagelijks miljoenen mailtjes verstuurd, zodat het totaal onmogelijk is dat iemand al die mailtjes kan lezen. Maar als je echt iets vertrouwelijks wil mailen, dan kan je gebruikmaken van een beveiligde maildienst als Hushmail **www.hushmail.com**. Let wel op: de ontvanger moet dan ook bij dezelfde dienst zitten, anders gaat je mailtje toch weer het onbeveiligde internet op. Denk je dat telefoneren veiliger is? Vergeet het maar; de telefoon kan gemakkelijk afgeluisterd worden. En omdat die technologie al jaren niet meer werd aangepast, kan je ervan uitgaan dat big brother zich daarin heeft gespecialiseerd.

➲ Ook via VoIP (Voice over IP) bel je onveilig, tenzij je Skype gebruikt: die dienst is volledig veilig (en nog niet gekraakt)...



Veilig bellen kan je met Skype.

10 Shoppen op internet is onveilig



Als je zelf naar PayPal of een webshop surft, is er geen probleem.

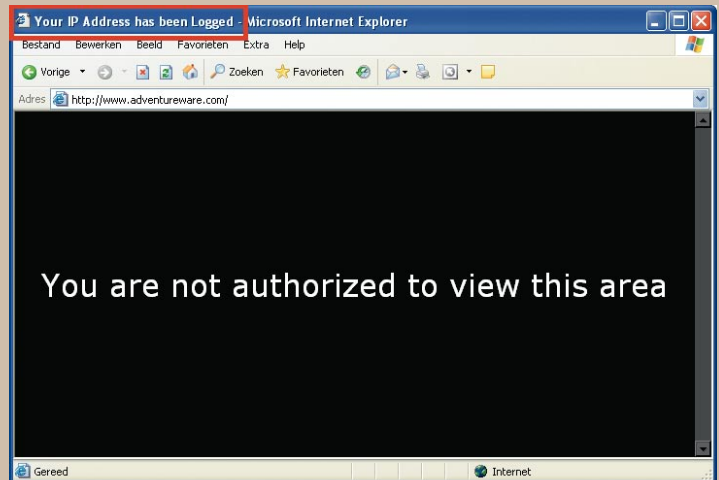
Internet gebruiken om informatie over bepaalde producten op te zoeken? Ja! Maar zelf shoppen op internet? Is dat wel veilig? Ik hoorde net nog dat dieven zomaar met je kredietkaartnummer aan de haal kunnen gaan! Ook dit is een (hardnekkig) fabeltje! Zorg ervoor dat je je gegevens doorgeeft op een site met encryptie (te herkennen aan **https://** in de url en het slotje onderaan je browser), en je zit goed. Kijk ook na of de verkoper wel betrouwbaar is, en klik nooit op links in e-mails of bepaalde vreemde websites. Je tikt beter zelf de url van de webshop in. Idem voor PayPal: betaal rechtstreeks vanuit eBay of surf zelf naar Paypal.

Sommige verkopers durven wel eens onveilig omspringen met kredietkaartnummers. Bepaalde shops slaan die namelijk op, en soms gebeurt dat niet beveiligd. Als zo'n site gehackt wordt, dan kunnen de hackers je kredietkaartnummer zien. Maar dat is nog maar heel zelden gebeurd. Bovendien ben je altijd verzekerd – een telefoontje naar je bank of kredietkaartmaatschappij, en je krijgt je geld terug. Het is trouwens véél onveiliger om je kredietkaart mee te geven aan de ober in een restaurant!

11 Iedereen weet wie je bent dankzij je IP-adres

Op bepaalde sites krijg je soms een pop-up te zien met als inhoud iets als Your IP address has been logged. Als je naar iets 'minder legaals' op zoek was, zoals muziekbestanden of cracks, denk je misschien dat de politie elk moment aan je deur kan staan. Dat klopt natuurlijk niet. Elke site kan je IP-adres loggen, ga daarvoor maar eens naar WhatIsMyIP www.whatismyip.com. Je IP-adres is inderdaad uniek, maar wijzigt regelmatig. Alleen jouw eigen provider weet wie op een bepaald moment een bepaald IP-adres had. En een bedrijf kan niet zomaar "even je provider bellen" om je adresgegevens te weten te komen.
Maar let op, want bedrijven kunnen wel een klacht indienen en juridische stappen ondernemen. En de rechter kan oordelen dat jouw gegevens vrijgegeven moeten worden. Dat is vroeger nog al gebeurd, bijvoorbeeld bij het verspreiden van illegale muziekbestanden. Maar door zelf ergens heen te surfen, weet de webmaster dus niet wie je bent.

➲ Tip: wil je echt anoniem surfen, gebruik dan een extra stukje software, zoals JAP http://anon.inf.tu-dresden.de. Je surft dan wel iets trager.



Dergelijke sites maken je alleen maar bang!

12 Websites kunnen nagaan of je pc besmet is

Als je aan het surfen bent op sites van bedenkelijk allooi, word je vaak bestookt met pop-upvenstertjes. Sommige daarvan beweren dat je computer besmet is. De webmasters van die sites zijn niet van gisteren, en maakten daarvoor een html-pagina die als twee druppels water op een Windows-foutmelding lijkt. Sommige pagina's detecteren zelfs met welke versie van Windows je werkt, zodat je foutmeldingen in je eigen taal krijgt. Dergelijke venstertjes bieden je ook meteen de oplossing voor het probleem: download een bepaald programmaatje. Krijg je dus een foutmelding, bekijk dan goed welk programma die foutmelding geeft. Als je Internet Explorer afsluit, dan verdwijnen die venstertjes meestal ook. Het is dus een goedkope reclametruc, en je computer is helemaal niet besmet! Een website kan namelijk onmogelijk in enkele seconden nagaan of je computer besmet is met een virus of met spyware!

➲ Een goede raad: sluit die venstertjes en scan je pc regelmatig met een antispywareprogramma als Windows Defender www.microsoft.com/athome/security/spyware/software/default.mspx of HitMan Pro www.hitmanpro.nl.



Een goedkope reclametruc...

CONCLUSIE

Urban legends zijn net dat: legendes, fabeltjes. Als je zelf de gebruikelijke voorzorgen neemt, dan gaat er niets mis. Met bovenstaande tips laat je je niet meer beïnvloeden door je betweterige neef, of door spam-mailtjes die je ervan proberen te overtuigen dat je eBay-account overgenomen is! ♦

13 Spyware stuurt al je mail en je kredietkaartnummer door



Een programma als AdAware maakt snel komaf met ongewenste spyware.

De meeste spyware wordt dan wel zonder jouw medeweten op je computer geïnstalleerd, maar verder doet zo'n spywareprogramma weinig. De 'beste' spyware kijkt na waar je heen surft, zodat je regelmatig reclame te zien krijgt over producten die je zouden kunnen interesseren. Maar zelfs dat gebeurt meestal niet. Sommige spyware 'kaapt' je browser door je startpagina aan te passen, zodat je hun zoekmachine gebruikt om op internet te zoeken. Maar dat verwijder je meestal snel met een antispywareprogramma als HitManPro www.hitmanpro.nl of AdAware www.lavasoft.de.
Echt 'goede' spyware zal je zelf niet zien: zo'n software nestelt zich ongezien op je pc en kan bijvoorbeeld al je toetsaanslagen bijhouden en doorsturen – dit is een zogenaamde 'keylogger'. Andere spyware neemt regelmatig screenshots en stuurt ze door per e-mail, ongezien. Een goed antispywareprogramma spoort zo'n software gelukkig snel op.